

Appl. No. : 09/712,398
Filed : November 14, 2000

REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claim 21 stand rejected under 35 U.S.C. 112, second paragraph, as indefinite. In response, claim 21 is canceled.

Claim 7 stands rejected under 35 U.S.C. 102(b) as allegedly being anticipated by Applebaum. Claims 8-14 stand rejected as allegedly being anticipated by Brody. These contentions are respectfully traversed. For reasons set forth herein, these rejections do not meet the Patent Office's burden of providing a prima facie showing of unpatentability.

Turning first to the response to arguments, the rejection states that claim 7 "does not indicate what exactly the software can do in the limited exception mode" or whether this "limited exception mode" is related to the user...". It is agreed that claim only defines that the limited exception mode is an "exception mode" and that it is "limited". Clearly, however, those words much mean that the mode is one for exceptions, and limited in some way. The rejection simply attempts to read these words out of the claim – which is quite clearly improper. Moreover, claim 7 as a whole CLEARLY establishes that the software is allowed to operate. The language of claim 36 of Applebaum does state restricting the access. From this, the rejection somehow reasons that the software is not prevented from operation. However, this contention is respectfully traversed. Nowhere does anything in Applebaum teach that the software can operate in any mode, much less a limited exception mode as claimed, without establishing that

Appl. No. : 09/712,398
Filed : November 14, 2000

the personal information agrees. The rejection does not meet the Patent Office's burden of providing a prima facie showing of unpatentability.

In responding to the arguments, the Patent Office states that Applicant's arguments regarding Brody, specifically that "nowhere is there any teaching or suggestion of 'obtaining misinformation as part of the installation routine', are not persuasive "because claim 8, in line 4 states: "obtaining the reference biometric information from an authorized user at the time of installing the software". However, this refers to Applicant's claim, not to anything in the prior art. The comment is quite simply inappropriate as part of a rejection. Nowhere does the prior art teach or suggest obtaining this kind of reference information at the time of installing the software, as claimed. Note that all of Brody's disclosure is consistent with the abstract of Brody which states that "personalization is incorporated into the software build and is delivered to the authorized user with embedded pre-existing personal information without requiring the user to input this information during setup or installation". The rejection attempts to read Brody in a way that would contradict this express teaching. This reading of Brody is improper. Brody's intent is to incorporate the personal information into the software build. This is exactly contrary to claim 8 and other similar claims.

The next comment in the rejection states correctly that claim 8 allows anyone to install the software, but quite simply attempts to confuse the issue. The EFFECT of the operation of claim 8 is that anyone can install the software. Certainly, that effect does not need to be claimed, since it follows naturally from the elements of the claim. While claim 8 does not define installing the software, it certainly defines that the reference

Appl. No. : 09/712,398
Filed : November 14, 2000

biometric is obtained "at the time of installing the software". This is not suggested by the prior art.

Claim 8 recites requesting a computer system to install a program and determining whether the program is verified for installation. Claim 8 recites obtaining "a reference biometric at the time of installing the software responsive to said determining..."

Therefore, this claim requires : a) determining whether the program is verified, and responsive to that determining, b) obtaining a reference biometric. Therefore, any user can install the software, but, whoever that user is, they must give the program a reference biometric at the time of installation. After installing, claim 8 recites that the program is allowed "to run normally only when biometric information is obtained which matches said reference biometric".

This is a very different system than that disclosed by Brody. Brody requires that each piece of software is "individually personalized for each customer separately to include personal information of the customer..."see for example paragraph 147 of Brody. Nowhere is there any teaching or suggestion of obtaining this information as part of the installation routine. Rather, Brody requires that each copy of the software is individually personalized. This is a very difficult system, since it may very well be difficult to mass-market software which has been individualized in the way that Brody teaches.

Brody admittedly teaches encryption and decryption in paragraph 152. However, note that the information is authenticated "prior to or during the software build". The

Appl. No. : 09/712,398
Filed : November 14, 2000

verification of the personalization is at run time, but the individualization is carried out during the software build, see generally the beginning of paragraph 152.

Therefore, this system only allows installation of the software by the person for whom the software was personalized. In contrast, claim 8 allows anyone to install the software. However, once installed, the software is matched with a reference biometric, and cannot later be used by anyone who does not match the reference biometric. This claimed process, even though it DOES NOT CLAIM THE WHOLE INSTALLATION, still produces advantages over Brody, and is nowhere taught or suggested by Brody.

Claim 9 is even further allowable, as it requires determining if the specified license has already been used. This would appear to be unnecessary in Brody who personalizes each copy of the program. Similar arguments apply for claim 10.

In rejecting claim 10, the rejection points attention to paragraphs like paragraphs 10 and 15 which describe how the prior art has recorded a unique serial number. However, Brody teaches personalizing each copy of the software, and therefore effectively teaches away from using such a unique serial number. Admittedly, Brody teaches finding and generating a unique identifier, but teaches nothing about using this to install the software so that the user's biometric information can be obtained at the time that the software is installed, as claimed.

Claim 19 was also rejected based on Brody. It is noted that Brody teaches using the personalization to determine whether the software can be installed, not whether it can be run after installation. Claim 19 specifies allowing the program to run in a specified way only when the reference biometric matches the current biometric. This is nowhere taught or suggested by Brody who only teaches verifying the information

Appl. No. : **09/712,398**
Filed : **November 14, 2000**

stream during installation, not at run time. The rejection refers to paragraph 153 as allegedly describing allowing the program to run in the specific way only when the reference biometric matches the current biometric. Paragraph 153 of Brody, however, teaches a different signature technique for the personal information. Paragraph 153 describes that this is detected "at run time" which, as emphasized throughout the remainder of Brody (e.g. C. paragraphs 147 and 152), refers to the time of installation.

Claim 3 was rejected over Applebaum in view of Brody. Applebaum does in fact teach a very different system than Brody, since Applebaum allows access to an appliance, not to a computer program. Applebaum teaches that biometric information can be obtained from the user and compared with biometric data that is stored to verify the identity. Paragraph 56 describes that encryption can be used. The encryption is described as being used to avoid the identity of the user being broadcast throughout the network. Other encryption is described in paragraphs 54 and 55.

Paragraph 54 describes that the encryption is carried out using the private key held by the server and that a public-key is provided to each user. However, nowhere is there any teaching or suggestion of doing this with a computer program, or any of the advantages that would be obtained from doing this with a computer program. Therefore, the hypothetical combination of these references is based on hindsight, and not on the teaching that the references define.

It is believed that this paper establishes the patentability of all of the pending claims. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be

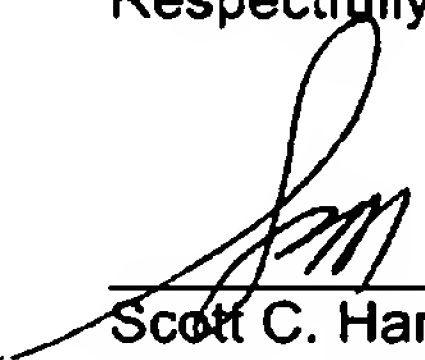
Appl. No. : 09/712,398
Filed : November 14, 2000

reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 11-15-04



Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082